

Sub
AB

Claimed is:

1. A secure wireless local area network (LAN), comprising:
a wireless device for use by a wireless device operator;
an access point connected to a wired LAN in communication with the wireless device
through an air channel for authenticating the wireless device; and
an authentication server connected to the wired LAN for providing the operator with
access to the wired LAN after authenticating the access point, the wireless device, and the
operator.
2. The secure wireless LAN of claim 1 wherein the access point includes a first
authentication device for sending a first authentication message to the wireless device, the
second authentication message including validating information about the access point.
3. The secure wireless LAN of claim 2 wherein the wireless device includes a
second authentication device for sending a second authentication message to the access point,
the first authentication message including validating information about the wireless device
and the operator.
4. The secure wireless LAN of claim 3 wherein the access point sends the first
and second authentication messages to the authentication server after authenticating the
wireless device.
5. The secure wireless LAN of claim 3 wherein the first and second
authentication devices are smart cards.
6. The secure wireless LAN of claim 1 including a control channel between the
access point and the authentication server for sending an authentication message between the
access point and the authentication server, the authentication message including validating
information about the access point, wireless device, and operator.
7. The secure wireless LAN of claim 6 including a data channel on the wired
LAN for sending data from the wireless device to any other device coupled to the wired
LAN, the data channel being enabled after the authentication message is validated by the

authentication server.

8. The secure wireless LAN of claim 6 wherein the communications between the wireless device and the access point and over the control channel is encrypted.

9. A secure wireless local area network (LAN), comprising:
a wireless means for use by a wireless device operator;
an access means connected to a wired LAN for authenticating the wireless means;
an authentication means connected to the wired LAN for enabling access to the wired LAN after authenticating the access means, the wireless device, and the operator.

10. The secure wireless LAN of claim 9 wherein the access means includes a first authentication means for generating, encrypting, and transmitting a first authentication message to the wireless device, the first authentication message including validating information about the access means.

11. The secure wireless LAN of claim 10 wherein the wireless device includes a second authentication means for generating, encrypting, and transmitting a second authentication message to the access means, the second authentication message including validating information about the wireless device and the operator.

12. The secure wireless LAN of claim 11 wherein the first authentication means transmits the first and second authentication messages to the authentication means after authenticating the wireless device.

13. The secure wireless LAN of claim 11 wherein the first and second authentication means are smart cards.

14. The secure wireless LAN of claim 9 including a control channel between the access means and the authentication means for sending an authentication message between the access means and the authentication means, the authentication message including validating information about the access means, the wireless device, and the operator.

15. The secure wireless LAN of claim 13 wherein communications between the wireless device and the access means and over the control channel are encrypted.

16. A method for operating a local area network (LAN), comprising:
5 generating a first authentication message including validating information about an access point connected to a wired LAN;
transmitting the first authentication message from the access point to a wireless device over a wireless channel;
validating the access point by analyzing the first authentication message;
10 generating a second authentication message including validating information about the wireless device and a wireless device operator;
transmitting the second authentication message from the wireless device to the access point;
validating the wireless device by analyzing the second authentication message;
15 transmitting the first and second authentication messages to an authentication server after validating the access point and the wireless device;
validating the operator; and
enabling a data channel between the wireless device and other devices on the wired LAN after validating the access point and the operator.

17. The method of claim 16 wherein transmitting the first authentication message includes transmitting information about the access point contained in a first authentication device.

18. The method of claim 17 wherein transmitting the second authentication message includes transmitting information about the wireless device and the operator contained in a second authentication device.

19. The method of claim 16 wherein transmitting the first and second authentication messages includes establishing a control channel between the access point and the authentication server.

A3

[illegible]